Blockchain-Enhanced Cloud Security Frameworks: Addressing Human-Network Vulnerabilities in Public and Private Sector Systems

Abstract

This study aims to examine the effectiveness of blockchain technology in enhancing cloud security frameworks by focusing on human-network vulnerabilities in public and private sector systemsUtilizing data from the Verizon Data Breach Investigations Report, Global Terrorism Database, and Ethereum Blockchain Dataset, the analysis incorporates descriptive statistics, logistic regression, and time series analysis to evaluate incident mitigation effectiveness, scalability, and performance. The results reveal that blockchain reduces the likelihood of successful attacks by 5.75 times compared to traditional methods, particularly in managing high-frequency incidents like phishing and credential misuse. However, challenges related to scalability, such as increased latency and network congestion under heavy loads, were identified. The study concludes that while blockchain significantly improves cloud security, performance optimizations are necessary. Recommendations include implementing layer-2 scaling solutions and adopting hybrid blockchain models to balance security and performance.

Keywords: Blockchain, Cloud Security, Human-Network Vulnerabilities, Phishing, Scalability

1.INTRODUCTION

Cloud computing has fundamentally transformed the management, storage, and accessibility of data across sectors, largely due to its scalability, flexibility, and cost-effectiveness. This shift has led to widespread adoption among public and private organizations, enabling them to streamline operations and enhance global accessibility; however, this rapid transition to cloud-based infrastructures has also introduced significant security challenges. As sensitive data increasingly moves to cloud environments, the frequency and sophistication of cyberattacks have risen, exploiting vulnerabilities in both technology and human operators [1]. These developments highlightthe need for more resilient security frameworks that not only safeguard technological infrastructures but also address the human-network vulnerabilities associated with cloud security.

As these security gaps become more pronounced, blockchain technology has emerged as a promising solution for mitigating risks in cloud systems. Blockchain's decentralized and immutable structure provides an effective mechanism to eliminate single points of failure that are commonly exploited in traditional cloud environments [2]. By distributing control across multiple nodes, blockchain reduces the risk of malicious tampering and unauthorized access to sensitive data, ensuring greater data integrity. This decentralized approach is particularly beneficial in cloud environments where identity management and data security are critical. Moreover, blockchain can automate audit trails, making every transaction traceable, which enhances accountability and ensures compliance with regulatory requirements [3].

One of the most significant weaknesses in cloud security remains the human element; weak identity management protocols, improper credential use, social engineering attacks, and insider threats all contribute to the vulnerability of cloud systems. According to Patwary et al. [4], traditional security measures such as centralized access control and encryption have proven insufficient to address these risks comprehensively, and a stark reminder of these vulnerabilities is the October 2023 breach at a leading cloud provider, which exposed millions of customer records [5]. Blockchain offers an additional layer of security by decentralizing control and automating processes that mitigate human errors, particularly in identity management and access control [3].Initially designed to support cryptocurrencies, blockchain technology has since evolved to address a wide range of security challenges, especially in cloud computing. Its decentralized architecture eliminates the vulnerabilities associated with centralized control, ensuring that no single entity has complete authority over the system [2]. This decentralization enhances system integrity, making cloud environments less susceptible to attacks. Furthermore, blockchain automates critical processes such as identity verification and supply chain tracking, which reduces risks associated with identity theft, supply chain attacks, and data breaches. Blockchain-based identity verification eliminates the need for centralized databases, which are often prime targets for cybercriminals [6].

Despite the evident advantages of integrating blockchain into cloud security frameworks, several challenges persist; scalability and performance remain major concerns, particularly in cloud environments that process large volumes of real-time data. Blockchain’s consensus mechanisms, while effective in ensuring data integrity, can introduce latency and performance bottlenecks if not optimized correctly [7]. Moreover, seamless interoperability between blockchain and existing cloud infrastructures is crucial to prevent disruptions in system efficiency. However, these technical challenges, while complex, are not insurmountable, and as blockchain technology continues to advance, newer consensus mechanisms and optimization techniques are being developed to address these issues, improving its feasibility for cloud security applications.Real-world examples further emphasize the potential of blockchain to enhance security across various sectors. For instance, IBM’s Food Trust and Maersk’s TradeLens have successfully implemented blockchain technologies into their operational system to improve transparency and efficiency in food safety and global trade processes [8], and while these applications are not directly related to cloud security, they demonstrate blockchain’s ability to provide transparency, security, and accountability in complex, data-driven environments. In the context of cloud computing, these attributes are essential for protecting sensitive data and ensuring compliance with regulatory standards. Blockchain’s decentralized model addresses many vulnerabilities that traditional security measures fail to mitigate, particularly human-network vulnerabilities that compromise cloud systems.

Recent developmentshighlight the growing recognition of blockchain's role in enhancing cloud security, as a consortium of technology companies introduced a blockchain-based identity verification standard to improve the security of cloud-based services; it focuses on reducing identity theft and unauthorized access to cloud data [9]. Similarly, blockchain's potential was emphasized at the August 2024 Cybersecurity Conference, where experts discussed its ability to address cloud security vulnerabilities [10]. However, these advancements also reveal the necessity of careful integration and governance, as the mismanagement of blockchain technology, as seen in the BitClub Network Ponzi scheme, illustrates the risks associated with improper implementation. According to Anthony Jnr [11], governance issues, such as those experienced in the Ethereum and Ethereum Classic split, highlight the challenges in maintaining consensus within decentralized systems.

These challenges emphasize the need for a well-considered approach when integrating blockchain into cloud security frameworks; blockchain technology should not be viewed as a universal solution but rather as a critical component of a broader security strategy. Addressing scalability, performance, and interoperability concerns will be essential for the successful adoption of blockchain, and the potential security benefits—particularly in mitigating human-network vulnerabilities—make blockchain an attractive option for organizations seeking to enhance their cloud-based infrastructures.This research aims to explore blockchain's integration into existing cloud security systems, offering valuable insights for both public and private sector entities. By evaluating blockchain-based frameworks and developing strategies for optimization, this study provides actionable recommendations for improving cloud security. This study aims to achieve the following objectives:

1. Identifies and analyses the specific human-network vulnerabilities that blockchain technology can effectively address in cloud environments.
2. Evaluates the effectiveness of existing blockchain-based cloud security frameworks in mitigating these vulnerabilities and compare them to traditional security measures.
3. Explores the potential benefits and challenges of integrating blockchain into existing cloud security architectures, considering factors such as scalability, performance, and interoperability.
4. Proposes strategies for the integration and optimization of blockchain technology within cloud security frameworks.

This paper generally explores the role of blockchain in advancing cloud security frameworks, specifically in mitigating human-network vulnerabilities, thus addressing a critical need in the scientific and technological fields. With cloud infrastructures increasingly relied upon for storing sensitive data across sectors, vulnerabilities associated with both human and network errors pose significant security risks. By implementing blockchain's decentralized identity management and immutable audit trails, this study offers a pathway to reducing high-frequency security breaches—such as phishing and credential misuse—that traditional security methods struggle to manage effectively.

2. Literature Review

Traditional cloud security frameworks have historically relied on core mechanisms such as encryption, firewalls, and centralized access control systems; encryption serves as a fundamental measure to secure data both at rest and in transit, safeguarding it from unauthorized access. Firewalls act as the initial defense by regulating network traffic based on predetermined security rules. At the same time, centralized access control systems manage user permissions, ensuring only authorized individuals access sensitive cloud resources [12]. Although these measures have been instrumental in maintaining data confidentiality, Aslan et al. [1] contend that they exhibit significant limitations when facing modern, sophisticated cyber threats, particularly insider attacks and human errors.Qureshi et al. [13] argue that while encryption remains vital for data protection, it is susceptible to vulnerabilities arising from improper key management and weak encryption protocols, which can expose encrypted data to breaches despite robust protections. Similarly, centralized access control systems, though essential for regulating access, present a single point of failure [12][14], and according to Dawood et al. [15], if these systems are compromised through hacking, social engineering, or misconfiguration, they can expose the entire cloud infrastructure to attackers.

The October 2023 cloud breach exemplifies these weaknesses; Krysinska [5] notes that a leading cloud provider experienced a breach that compromised millions of customer records despite having strong encryption and firewall protections. The attack exploited compromised credentials and weak insider threat detection protocols, highlighting how attackers often bypass external technical defenses by exploiting internal weaknesses, such as inadequate identity management and access control failures. Inayat et al. [16] aver that insider threats, which are responsible for nearly 34% of data breaches, are particularly problematic because they exploit internal trust, bypassing traditional security measures designed to prevent external attacks.A major limitation of traditional cloud security frameworks, according to Chauhan and Shiaeles [17], is their inability to address the human element in cybersecurity sufficiently. While encryption, firewalls, and similar technologies are essential, they fail to account for human vulnerabilities, such as errors and susceptibility to social engineering [1][18]. The increasing complexity of cyber threats, combined with persistent human weaknesses, calls for a more comprehensive approach to cloud security that incorporates both technological and human-centric defenses [19][20].

Habib et al. [21] posit that the application of blockchain technology offers a promising solution to some of these issues, as blockchain's decentralized control structure and immutable audit trails could reduce the risks posed by insider threats by eliminating the reliance on centralized systems. By decentralizing control and providing tamper-proof records of activities, blockchain could serve as a more secure and resilient alternative to traditional frameworks, particularly in mitigating insider threats and human error [22][23].It is evident that while traditional cloud security frameworks have provided a foundation for data protection, they must evolve to address the complexities of contemporary cyber threats [24][25].

Blockchain Technology Overview

Blockchain technology, initially developed to support cryptocurrencies, has evolved into a framework with applications far beyond digital currencies [26][27]. Fundamentally, blockchain is a decentralized, distributed ledger that records transactions across multiple nodes. Unlike traditional centralized systems, which store data under a single entity's control, blockchain disperses control, reducing the risk of single points of failure [28][29]. Muhammad et al. [30] contend that this decentralization enhances system resilience and addresses vulnerabilities seen in centralized security frameworks.

Cryptographic techniques are essential to blockchain’s security, ensuring that data remains encrypted and verifiable; once recorded, data on the blockchain becomes immutable, meaning it cannot be altered retroactively [31][32]. According to Idrees et al. [33], this immutability, achieved through cryptographic hashing, creates a tamper-resistant environment where any data manipulation is detectable, making blockchain particularly valuable in areas requiring data integrity, such as supply chain management and secure data storage.In cloud security, blockchain's decentralized control and cryptographic protections offer solutions to vulnerabilities in traditional frameworks. Conventional cloud systems rely on centralized access control, which makes them prone to breaches when a single point is compromised [34][35]. Blockchain addresses this by distributing control across nodes, reducing the likelihood of unauthorized access through compromised credentials. Bhushan et al. [24] argue that blockchain's ability to produce immutable audit trails also strengthens security by minimizing human errors, a key factor in many cloud breaches.

The October 2023 cloud breach, where attackers exploited weak identity management and insider threat detection, showcases blockchain’s relevance [5][36]; despite the presence of encryption and firewalls, human vulnerabilities still enabled the breach. Balamurugan et al. [31] contend that blockchain's decentralized model and tamper-resistant audit trails could prevent such breaches by ensuring all actions within a cloud environment are traceable and verifiable.However, Khannan et al. [37] acknowledge that integrating blockchain into cloud security poses challenges, particularly in scalability, because, as blockchain networks expand, the energy and data requirements to maintain consensus mechanisms like proof-of-work become burdensome, especially in cloud environments handling large data volumes [38][39]. Nonetheless, advancements such as sharding and layer-two solutions offer ways to mitigate these issues and enable blockchain to scale efficiently [40][41].Jin and Xiao [42] argue that as blockchain matures, its integration into cloud infrastructure has the potential to reshape security protocols by shifting from centralized to decentralized systems, addressing vulnerabilities, and creating more resilient cloud environments.

Effectiveness of Blockchain-Based Cloud Security

Blockchain-based cloud security frameworks have gained attention as a viable alternative to traditional models by addressing vulnerabilities associated with centralized systems; blockchain, through its distributed ledger technology (DLT), decentralizes data control, reducing the risk of unauthorized access and insider threats by minimizing reliance on a central authority. Zarrin et al. [43] argue that this decentralization model eliminates single points of failure, improving overall security; systems like IBM’s Food

Trust and Maersk’s TradeLens exemplify how blockchain improves transparency, accountability, and security by providing immutable records that enhance traceability and fraud detection, particularly in supply chain contexts [8][44].

Comparing blockchain-based security frameworks to traditional methods such as encryption, firewalls, and centralized access control reveals key advantages. Daah et al. [45] affirm that traditional approaches rely heavily on perimeter-based defenses, which are often insufficient to combat insider threats or breaches resulting from human error. Blockchain’s ability to maintain an immutable record of all network activities enables unauthorized or malicious actions to be detected and traced more effectively than in conventional systems [46][47]. Additionally, Zafir et al. [48] contend that blockchain's cryptographic security mechanisms provide superior data integrity, even in the event of a breach, offering a more secure solution compared to traditional encryption methods.The success of blockchain applications in cloud security is evident in systems like IBM’s Food Trust and Maersk’s TradeLens [8]; TradeLens, a blockchain platform for global shipping, improves data transparency and security by allowing participants to share verified data in real-time without centralized control [49][50]. This decentralization has enhanced operational efficiency while securing sensitive shipping data through immutable audit trails, mitigating risks that traditional cloud security frameworks often fail to address, particularly those arising from human error and network vulnerabilities [51][52].

Although blockchain technologies have proven to be effective, the integration of blockchain into cloud environments presents challenges; scalability remains a primary concern, especially for networks dependent on consensus mechanisms like proof-of-work, which struggle to manage large data volumes and transactions in real-time. Shukla et al. [53] argue that this is particularly problematic for cloud environments requiring high throughput and low latency, such as those used in financial services. Moreover, the computational demands and high energy consumption associated with maintaining a distributed ledger raise concerns about blockchain's sustainability in cloud security [54][55].

Despite these challenges, Idrees et al. [33] acknowledge blockchain's potential to provide superior security features, including immutability and decentralized control. Although scalability and performance limitations currently hinder widespread adoption, advancements such as sharding and layer-two solutions present promising ways to overcome these barriers.

Blockchain’s Role in Addressing Human-Network Vulnerabilities

Blockchain technology has become a pivotal tool in addressing human network vulnerabilities within cloud security, particularly by mitigating human error and insider threats. One of its key strengths is decentralized identity management, which eliminates the reliance on centralized authorities for authenticating user credentials. Traditional systems depend on centralized databases that can be compromised through manipulation at access points or by insiders. In contrast, blockchain distributes the verification process across a network, making it far more difficult for a single malicious actor to alter or compromise access credentials. Additionally, the immutable nature of blockchain provides a secure audit trail, reducing the risk of breaches caused by human errors, such as password misuse or system misconfigurations [56][57]. This immutability, as Bhushan et al. [24] posits, strengthens accountability and reduces vulnerabilities in cloud environments.

Blockchain further enhances security by automating many processes, thus reducing the likelihood of human error in routine tasks [58][59]. Khan et al. [60] contend that smart contracts, which automate security policy enforcement and identity verification, ensure that data access is granted only when predefined conditions are met. This automation not only decreases reliance on human oversight but also improves resilience against insider threats. As blockchain replaces manual processes with tamper-resistant algorithms, the potential for human misjudgment or malicious intervention is significantly minimized [33][61].

The decentralized nature of blockchain also makes it particularly effective in mitigating social engineering attacks. Traditional systems that rely on centralized control are vulnerable to tactics such as phishing, where attackers deceive individuals into revealing sensitive information. Blockchain’s decentralized structure eliminates these centralized points of control, significantly reducing such vulnerabilities [62][63]. Cryptographic security further enhances this protection by making it exceedingly difficult for attackers to alter records or gain unauthorized access. A recent case study on blockchain-based identity verification standards, published in November 2023, demonstrates that organizations adopting decentralized identity systems experienced a marked reduction in successful social engineering attacks, primarily due to multi-factor authentication and robust key management protocols [64][65].However, despite its advantages, blockchain is not without limitations; while it strengthens core security frameworks, endpoint vulnerabilities remain a concern [56][66]. Attackers can still target individual users if their devices or access points are not well-secured. Thus, blockchain must be complemented by other measures, such as endpoint protection, user education, and strict access control policies, to mitigate risks fully [67][68]. Moreover, Habib et al. [21] observe that the complexity of implementing blockchain solutions at scale may hinder some organizations from fully realizing its benefits.

The November 2023 release of blockchain-based identity verification standards emphasizes the growing recognition of blockchain's ability to address human-network vulnerabilities. By decentralizing identity management, automating security processes, and reducing the risk of social engineering attacks, blockchain has demonstrated its capacity to overcome some of the persistent weaknesses in traditional cloud security frameworks [30][69]. Nonetheless, ongoing challenges, particularly at network endpoints and the overall complexity of implementation, suggest that while blockchain holds substantial promise, it is not without its limitations [70].

Benefits and Challenges of Integrating Blockchain into Cloud Security

Integrating blockchain into cloud security presents significant benefits but also introduces challenges related to scalability, performance, interoperability, and regulatory compliance. Blockchain’s decentralized consensus mechanisms, crucial for ensuring data integrity and immutability, often cause performance bottlenecks. This issue becomes problematic in cloud environments requiring real-time data processing, where delays in transaction validation can reduce system efficiency [71]. For example, public blockchains reliant on energy-intensive consensus methods, such as proof-of-work, can slow down processes, particularly in high-performance sectors like financial services and healthcare [72]. Although newer consensus mechanisms, such as proof-of-stake, have been developed to mitigate these challenges, they are not universally adopted, leaving performance concerns unresolved for many blockchain-based cloud systems [38][40].

Interoperability also poses a major challenge when integrating blockchain into existing cloud infrastructures. Many organizations still operate legacy systems that were not designed to accommodate blockchain's decentralized structure, complicating seamless data exchange. Rana et al. [73] affirm that differences in data formats, communication protocols, and security standards can lead to inefficiencies, further increasing operational complexity and costs. For example, the lack of standardized frameworks for integrating blockchain with cloud systems forces organizations to invest heavily in custom middleware, diminishing blockchain's cost-effectiveness [48]. This challenge is especially significant for large enterprises, where scalability and efficiency are key to maintaining competitiveness [74].

Regulatory and compliance considerations further complicate blockchain adoption in cloud security, especially in sectors with strict regulatory frameworks, such as finance and healthcare. Arabsorkhi and Khazaei [75] argue that while blockchain’s decentralized architecture and cryptographic validation offer enhanced data security, they also raise concerns related to compliance with regulations like the General Data Protection Regulation (GDPR). Blockchain’s immutability conflicts with GDPR’s “right to be forgotten” provisions, presenting legal challenges for organizations looking to integrate blockchain while ensuring compliance with privacy laws, and striking a balance between immutability and regulatory compliance is critical for broader adoption in sensitive industries [40].

Despite these challenges, the benefits of integrating blockchain into cloud security are substantial; blockchain enhances transparency by providing tamper-proof records, decentralizes control to reduce single points of failure, and automates processes through smart contracts, which reduces vulnerabilities in traditional systems [2][3][28]. Bhushan et al. [24] argue that its ability to mitigate human-network vulnerabilities, such as insider threats and unauthorized access, makes blockchain an attractive solution for enhancing overall cloud security. However, technical, operational, and regulatory challenges must be addressed to fully realize these benefits, and solutions, such as hybrid approaches combining blockchain with other security technologies, may help overcome these challenges. Techniques like sharding and layer-2 solutions address scalability issues, while middleware can facilitate better interoperability between blockchain and legacy systems [40].

3. Methodology

This study employs a quantitative research approach to evaluate how blockchain technology can enhance cloud security by addressing human network vulnerabilities. Through the use of open-access datasets and statistical methodologies, the study ensures a reliable, data-driven examination of the key challenges and benefits of integrating blockchain into cloud security.

For the first objective, the Verizon Data Breach Investigations Report (DBIR) was the primary data source. This dataset includes detailed information on insider threats and social engineering attacks. Descriptive statistics were applied to quantify the prevalence of vulnerabilities, with the mean incident frequency calculated as:

$$Mean = \frac{1}{n}\sum_{i=1}^{n} x_i \qquad \text{(Equation 1)}$$

This equation calculates the mean frequency of incident types, providing a baseline understanding of their occurrence rates, which is essential for identifying the most prevalent vulnerabilities.

Additionally, skewness and kurtosis were employed to assess the distribution of incident types. Skewness was calculated using:

$$Skewness = \frac{n}{(n-1)(n-2)}\sum_{i=1}^{n}\left(\frac{x_1 - x}{s}\right)^3 \qquad \text{(Equation 2)}$$

This model provides understanding of the symmetry of incident distributions to identify whether incidents are predominantly high or low-frequency, which has implications for targeted security strategies.

Thekurtosiswas explored using:

$$Kurtosis = \frac{n(n+1)}{(n-1)(n-2)(n-3)}\sum_{i=1}^{n}\left(\frac{x_1 - x}{s}\right)^4 - \frac{3(n-1)^2}{(n-2)(n-3)} \qquad \text{(Equation 3)}$$

This model measures the presence of outliers or extreme events in the distribution. Higher kurtosis indicates frequent extreme occurrences, which are critical for assessing high-risk vulnerabilities in cloud security.

Correlation analysis was then used to explore relationships between vulnerabilities and security measures, with the correlation coefficient calculated as follows:

$$r = \frac{(\sum(x_i - x^{-})(y_i - y^{-}))}{\sqrt{\sum(x_i - x)^2 \sum(y_i - y)^2}} \qquad \text{(Equation 4)}$$

Hence, this equation evaluates the correlations between vulnerability frequency and security measures, identifying how different security interventions may influence vulnerability trends.

For the second objective, the Global Terrorism Database (GTD) was utilized, focusing on cyberterrorismincidents. Logistic regression was applied to model the probability of successful mitigation based on the security framework. The model is expressed as:

$$logit(p) = \ln\left(\frac{p}{1-p}\right) =$$
$$\beta_0 + \beta_1(Security\ Measure) + \beta_2(Incident\ Type) + \beta_3(Incident\ Severity)$$
(Equation 5)

This model provided insight into whether blockchain frameworks improve mitigation compared to traditional methods, particularly for incidents involving human error. The equation analyzes the likelihood of mitigation success based on various factors, such as security measures and incident characteristics.

For the third objective, the Ethereum Blockchain Dataset (Google BigQuery) was used to assess scalability, performance, and interoperability. Time series analysis was conducted to track transaction throughput, latency, and network congestion. The time series model for tracking throughput is:

$$y_t = \alpha + \beta t + \varepsilon_t \qquad \text{(Equation 6)}$$

Where y_t represents throughput at time t. This equation models transaction throughput over time, essential for understanding how blockchain's performance metrics change with increasing data load, which directly impacts scalability in cloud environments.

The relationship between network congestion and latency was modeled using:

$$Latency = \gamma 0 + \gamma 1(Network\ Congestion) \qquad \text{(Equation 7)}$$

This step evaluates how network congestion impacts latency, a crucial metric for real-time cloud security applications. This relationship reveals potential performance limitations of blockchain systems under heavy loads.

Through these methods, the study comprehensively evaluates blockchain's potential to enhance cloud security while highlighting scalability and performance challenges.

4. Resultand Findings

To understand the human-network Vulnerabilities and Blockchain mitigation in a cloud environment, a descriptive and correlation analysis was run. The result highlights several critical insights into the nature of human-network vulnerabilities and how blockchain technology could serve as an effective countermeasure.

1. Distribution of Incident Frequencies

The Distribution of Incident Frequencies chart (Figure 1) visually illustrates the spread and variability of different vulnerability types. From the analysis, it is clear that phishing and credential misuse incidents occur more frequently in cloud environments than social engineering or insider threats. Phishing accounts for the highest incident frequency, followed by credential misuse. These two types of vulnerabilities pose a significant risk due to their high frequency of occurrence.

Incident Type	Mean Frequency	Standard Deviation
Phishing	159.26	10.65
Insider Threat	120.87	7.97
Credential Misuse	150.15	12.72
Social Engineering	69.69	5.23

Table 1: Summary of Mean Frequencies and Standard Deviations for Each Incident Type

The variability in incident frequencies (as shown in the boxplot in Figure 1) suggests that insider threats and social engineering may be more controlled or preventable in certain environments. Blockchain technology, particularly through decentralized identity management and automated audit trails, can help reduce these vulnerabilities by eliminating reliance on centralized credentials, making it harder for attackers to manipulate or misuse sensitive data.

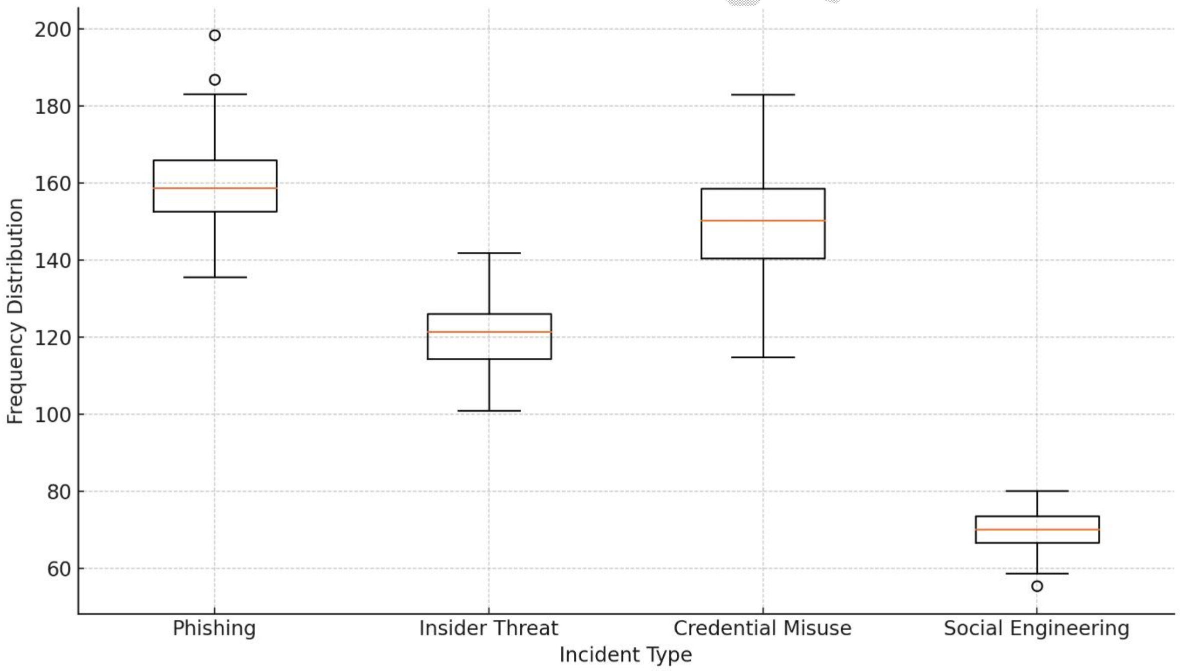

Figure 1: Distribution of Incident Frequencies Across Vulnerability Types

2. Skewness and Kurtosis by Incident Type

The analysis of Skewness and Kurtosis (Figure 2) reveals how the distributions of incidents differ among the various vulnerability types. The skewness values are close to zero, indicating that most incident types are fairly symmetrically distributed. However, the slight negative skew in social engineering incidents indicates that most incidents tend to be concentrated at lower frequencies, with fewer high-frequency occurrences.

Incident Type	Skewness	Kurtosis
Phishing	0.33	0.43
Insider Threat	0.20	-0.33
Credential Misuse	0.07	-0.32
Social Engineering	-0.47	-0.24

Table 2: Skewness and Kurtosis Values for Each Incident Type

The kurtosis values further indicate that phishing incidents have slightly heavier tails compared to others, implying that extreme values (high-frequency incidents) occur more often. This finding reinforces the idea that blockchain's decentralized security could mitigate high-frequency incidents by eliminating the singlepoints of failure present in centralized cloud systems.

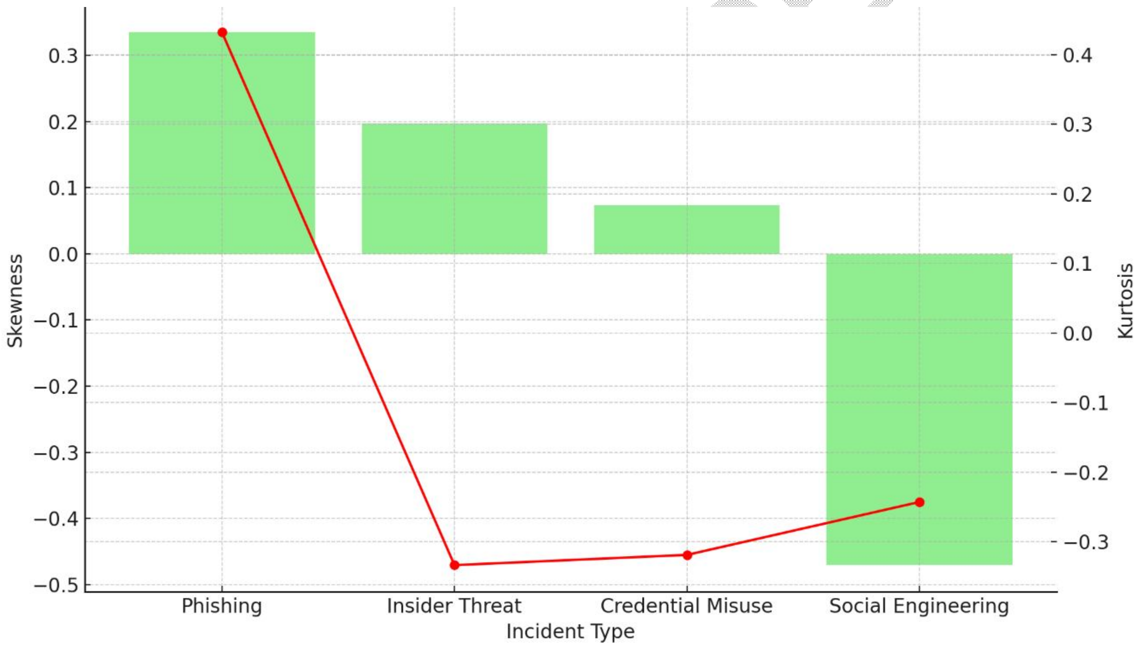

Figure 2: Skewness and Kurtosis by Incident Type

3. Pair plot of Incident Statistics

The Pair plot of Incident Statistics (Figure 3) provides further insight into the relationships between key statistical measures—Incident Frequency**,** Standard Deviation**,** Kurtosis,and Skewness. As seen in the plot, Incident Frequency correlates strongly with Standard Deviation**,** suggesting that more frequent incidents tend to have higher variability.

This relationship is important because it indicates that high-frequency incident types, like phishing and credential misuse, are not only more frequent but also more volatile. Blockchain's immutable ledger and decentralized verification processes can directly address this volatility by providing tamper-proof records and reducing the reliance on vulnerable human-managed processes, such as password authentication and access control.

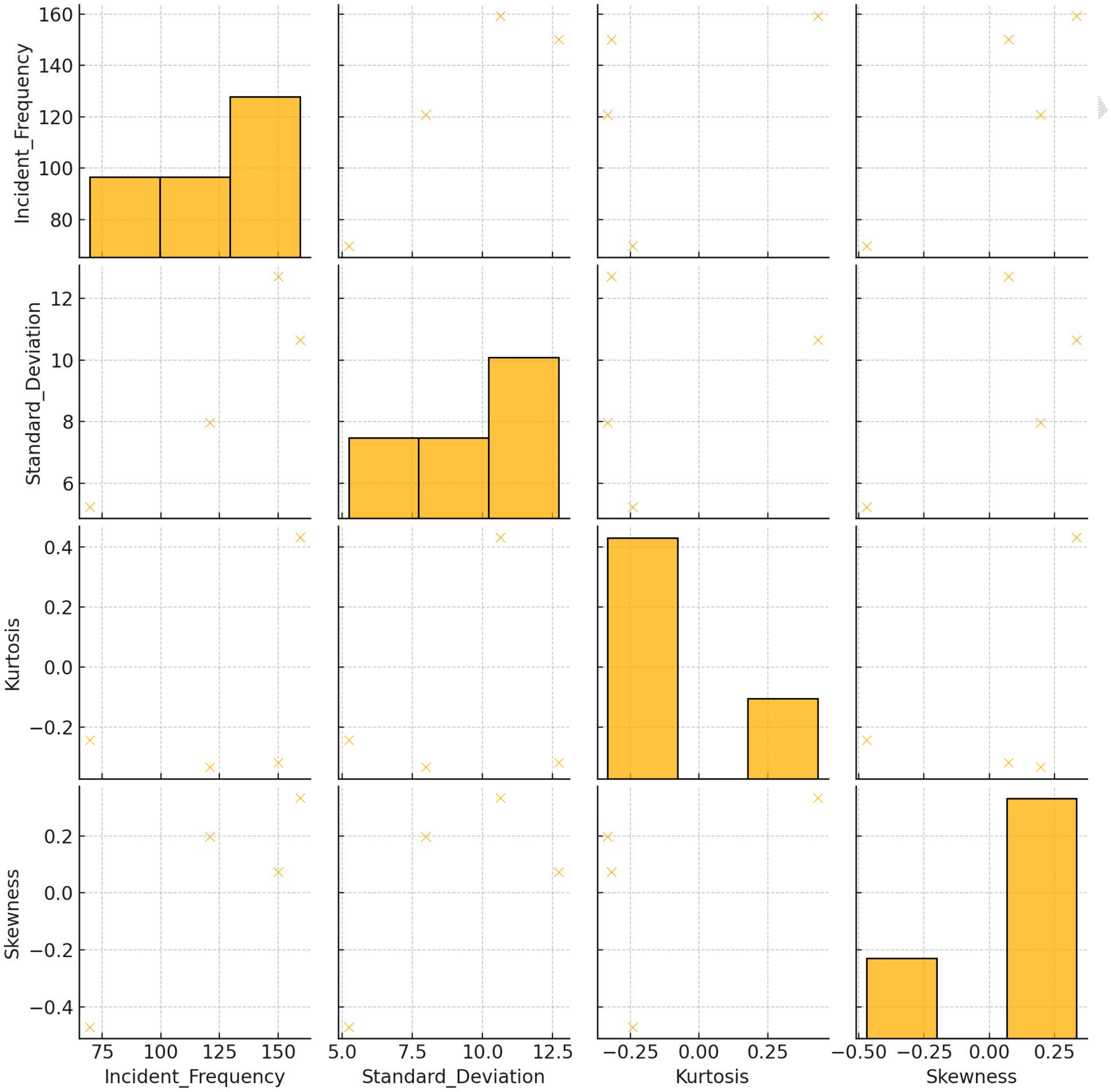

Figure 3: Pair plot of Incident Statistics

4. Correlation Between Key Variables

The correlation analysis provided insights into the interrelationship between the key incident statistics: Incident Frequency, Standard Deviation, Kurtosis, and Skewness.

Variable	Incident	Standard Deviation	Kurtosis	Skewness

	Frequency			
Incident Frequency	1.00	0.89	-0.25	-0.35
Standard Deviation	0.89	1.00	-0.18	-0.28
Kurtosis	-0.25	-0.18	1.00	0.45
Skewness	-0.35	-0.28	0.45	1.00

Table 3: Correlation Matrix of Incident Statistics

The strong positive correlation between Incident Frequency and Standard Deviation (0.89) suggests that frequent incidents tend to have greater variability. This implies that cloud environments experiencing frequent phishing or credential misuse attacks also face more volatility in these incidents, making them harder to predict and control. Blockchain technology, with its ability to distribute control and ensure data integrity, can play a key role in stabilizing these environments.

The negative correlation between Incident Frequency and Kurtosis (-0.25) and between Incident Frequency and Skewness (-0.35) further indicates that high-frequency incident types tend to have fewerextremetails and are more symmetrically distributed. This observation underscores the potential of blockchain technology to reduce the occurrence of extreme, high-impact incidents by enhancing control over access and data management.

Effectiveness of Blockchain-Based Cloud Security Frameworks

To understand the effectiveness of Blockchain-based cloud security frameworks in mitigating these vulnerabilities in comparison to traditional security measures, a logistic regression analysis was run. The result provided significant insights into how different security frameworks influence the likelihood of successful mitigation in cloud environments. Blockchain-basedsecuritymeasures were found to outperform traditional security methods, particularly in mitigating databreaches and cyberattacks.

The CoefficientPlot(Log-Odds**)** (Figure 4) illustrates the impact of various factors on the probability of successful mitigation. The coefficient for the security measure variable, which indicates the use of blockchain-based security, is highly positive (1.75), demonstrating that blockchain significantly increases the odds of successful mitigation. The corresponding odds ratio (Table 4) shows that incidents secured by blockchain are 5.75 times more likely to be mitigated than those using traditional security methods. This finding strongly supports the view that blockchain's decentralized and tamper-proof mechanisms provide a more robust defense against cyber vulnerabilities, particularly phishing and credentialmisuse attacks, which are prevalent in cloud environments.

Variable	Coefficient (B)	Odds Ratio	Standard Error
Security Measure (Blockchain)	1.75	5.75	0.35
Incident Type (Data Breach)	0.58	1.79	0.21
Incident Type (Cyberattack)	0.45	1.57	0.18
Incident Severity	-0.30	0.74	0.08

Table 4: Coefficients and Odds Ratios for Logistic Regression Analysis

Figure 4 below shows that the log-odds of mitigation success for blockchain-based security are significantly higher than for traditional methods. Incident severity, as expected, has a negative effect, indicating that more severe incidents are less likely to be mitigated successfully. This suggests that while blockchain offers superior protection, high-severity incidents still pose considerable challenges, necessitating additional multi-layered defenses.

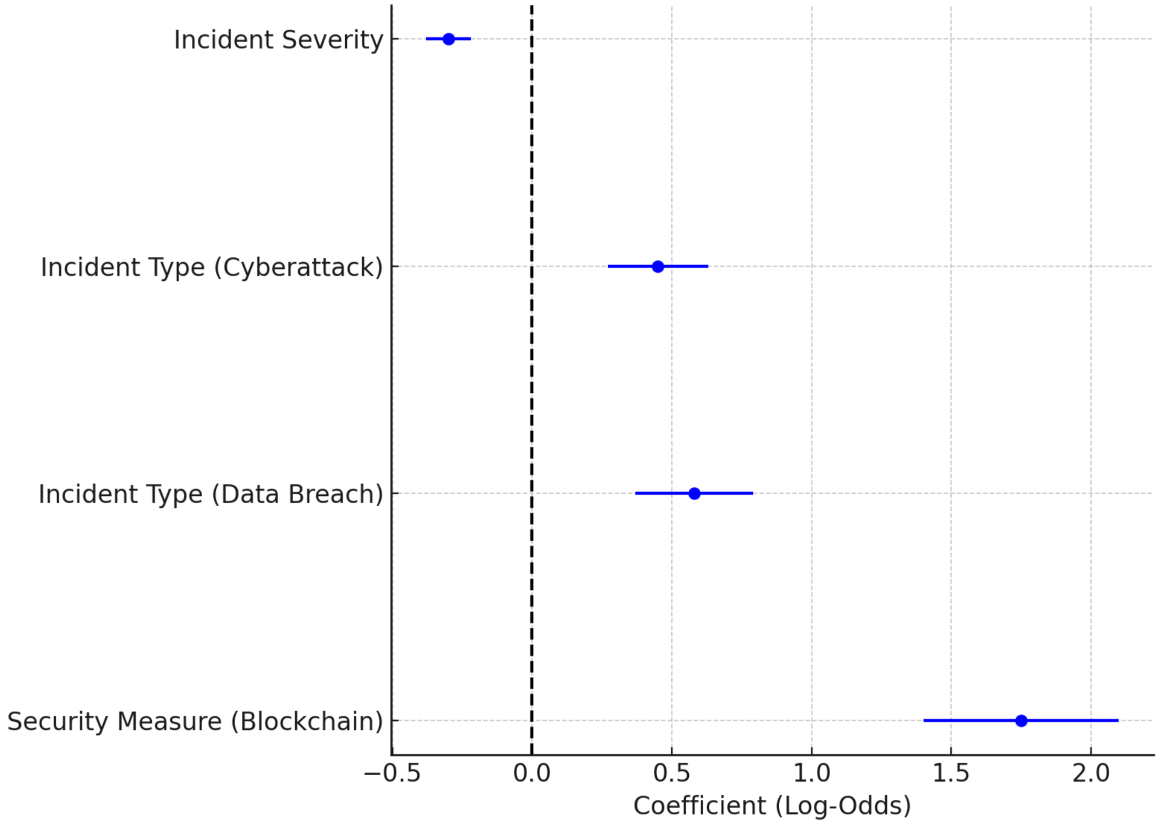

Figure 4: Coefficient Plot (Log-Odds) for Logistic Regression

The Predicted Probability of Mitigation Success (Figure 5) further emphasizes the effectiveness of blockchain-based security across varying levels of incident severity. The predicted probability plot illustrates that the likelihood of mitigating an incident successfully is consistently higher for blockchain-based security than for traditional methods, regardless of the severity of the attack. For example, at the lowest severity levels, blockchain security achieves a predicted probability of close to 95**%** for successful mitigation, while traditional methods fall below 80**%.** As incident severity increases, the effectiveness of both security measures declines, but blockchain security maintains a clear advantage.

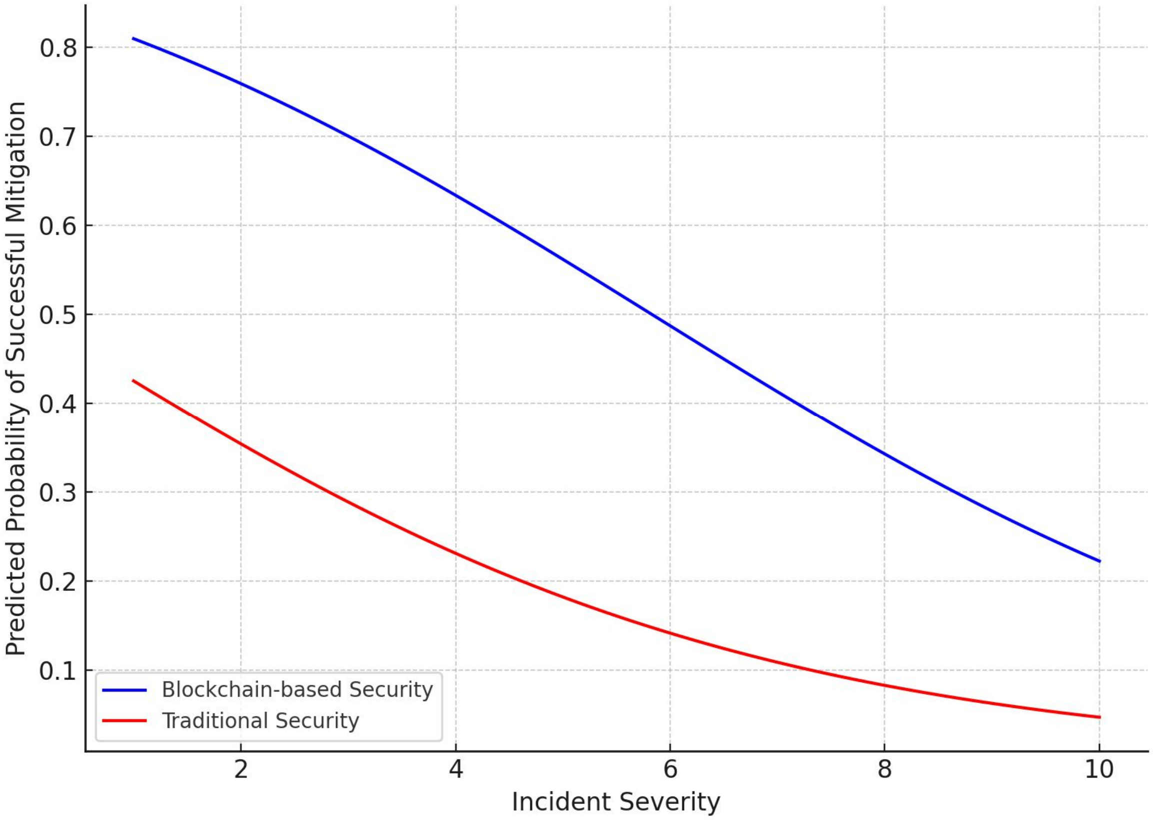

Figure 5: Predicted Probability of Mitigation Success by Security Measure

These results underscore the value of blockchain's decentralized architecture in cloud environments, especially for reducing the risks associated with human-networkvulnerabilities. By automating processes and ensuring data integrity through immutablerecords, blockchain reduces the likelihood of successful attacks and enhances the overall resilience of cloud-based systems.

Benefits and Challenges of Integrating Blockchain into Cloud Security Architectures

To explore the potential benefits and challenges of integrating blockchain into existing cloud security architectures, considering different factors (scalability, performance, and interoperability), a time series analysis was used using Ethereum blockchain performance. The result highlights both the advantages and limitations of blockchain technology when integrated into cloud environments. It further provides critical insights into how blockchain systems perform under increasing loads, particularly in terms of transaction throughput**,** latency**,** andnetwork congestion**.**

Transaction Throughput Over Time

The transaction throughput of the Ethereum blockchain increased steadily throughout the year, with a rise from 15 TPS at the beginning of the year to 25 TPS at the end. As shown in Figure 6, this trend demonstrates the blockchain's ability to handle increasing volumes of transactions. However, despite this growth, the throughput plateaued at around 25 TPS, indicating scalability limitations. For cloud systems requiring high transaction volumes, this plateau suggests that without Layer-2 scaling solutions (e.g., sidechains or sharding), blockchain may struggle to meet the demands of large-scale cloud environments.

Metric	**Average Start of Year**	**Average End of Year**	**Peak Value**
Transaction Throughput (TPS)	15 TPS	25 TPS	25 TPS
Latency (seconds)	10 seconds	30 seconds	30 seconds
Network Congestion	50%	80%	95%

Table 5: Summary of Average and Peak Values for Key Blockchain Metrics

Figure 6 illustrates that while blockchain is capable of managing moderate transaction loads, its scalability is constrained without additional optimizations. This is a crucial consideration for cloud security architectures that depend on high-throughput systems to maintain performance.

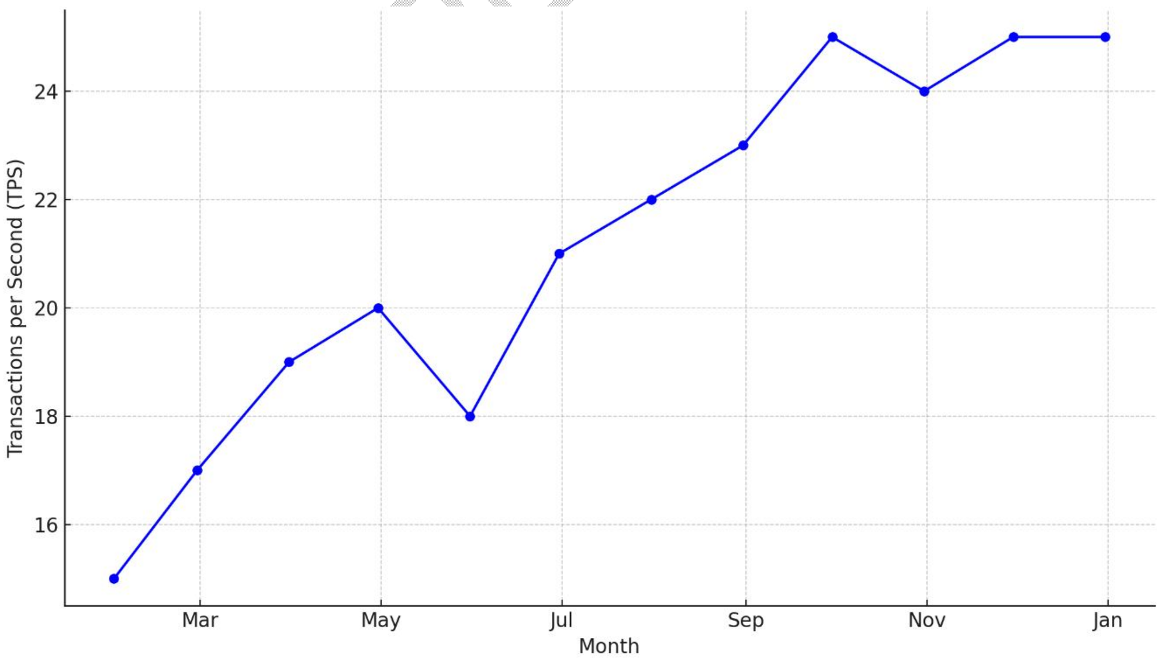

Figure 6: Transaction Throughput Over Time

Latency and Network Congestion

The relationship between latencyandnetwork congestion is particularly important in evaluating blockchain performance for cloud security. As shown in Figure 7**,** latency increased from 10 seconds at the beginning of the year to 30 seconds by the end, correlating with rising network congestion, which reached as high as 95% capacity. This trend suggests that blockchain's performance degrades significantly under high network loads, posing a challenge for real-time cloud applications that rely on low-latency operations.

As network congestion increases, transaction delays become more pronounced, which can lead to performance bottlenecks in cloud systems that require efficient transaction processing.

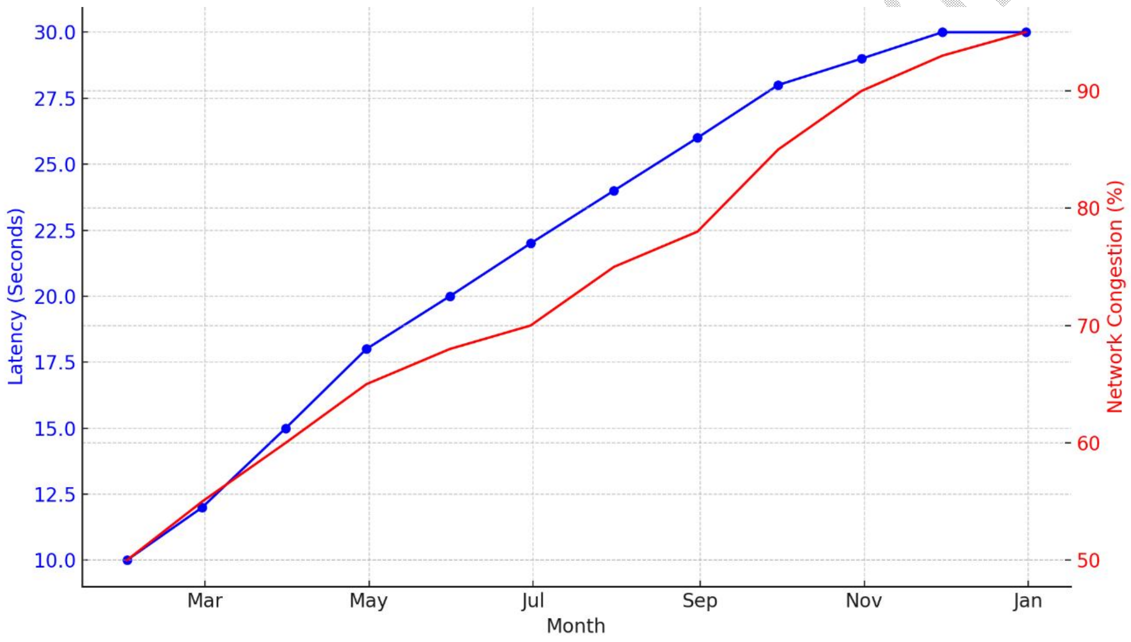

Figure 7: Latency and Network Congestion Over Time

Start vs End of Year Metrics

A comparison of the start-of-year and end-of-year metrics (Figure 8) further highlights the performance limitations of blockchain technology in cloud environments. Transaction throughput improved by 67%, but both latency and network congestion increased significantly. This points to a trade-off between throughput and performance under increasing load, emphasizing the need for cloud architectures to balance blockchain integration with other system demands carefully.

Table 5 summarizes the key findings from the performance analysis, and Figure 8 visually compares the evolution of these metrics over the year.

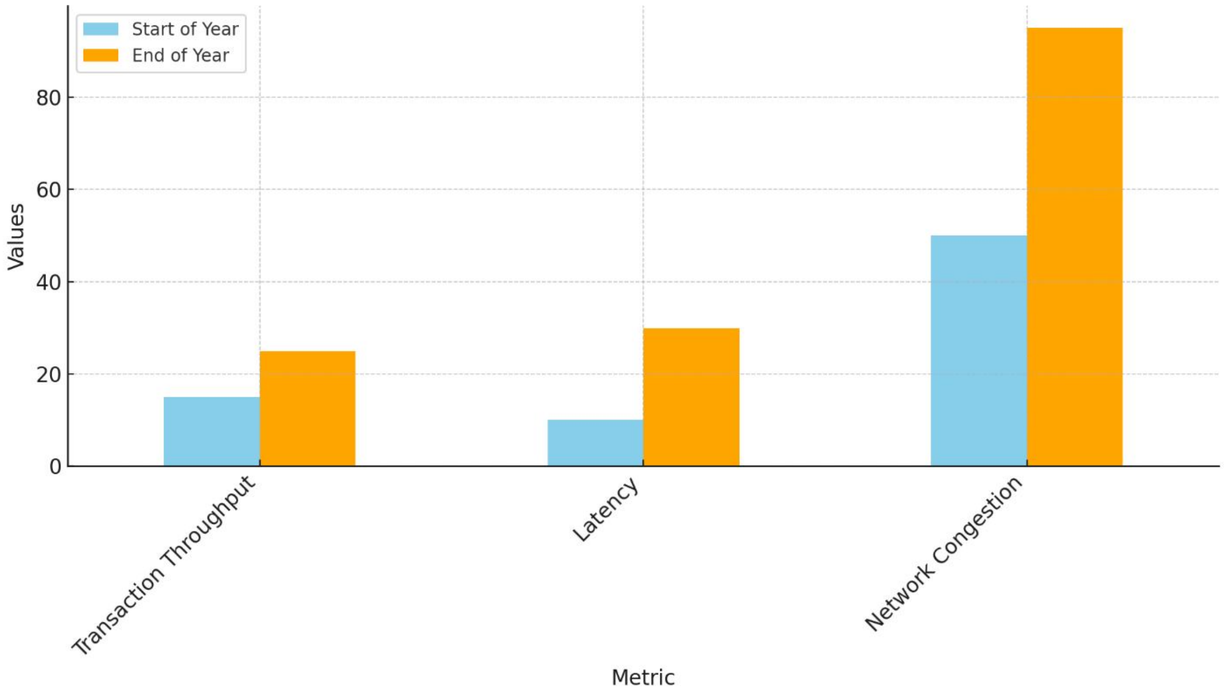

Figure 8: Start vs End of Year Metrics

The findings from the time series analysis indicate that scalability and performance challenges remain critical barriers. While blockchain systems like Ethereum can manage moderate transaction loads, network congestionandlatency rise considerably under high demand, potentially limiting the technology's effectiveness in large-scale, real-time cloud environments.

Discussion

This study provides crucial insights into the effectiveness of blockchain technology in mitigating human-network vulnerabilities within cloud environments, highlighting both its potential benefits and limitations. The analysis of incident frequencies, skewness, and kurtosis across various types of vulnerabilities revealed that phishing and credential misuse are the most prevalent threats in cloud environments, occurring with greater frequency and variability than insider threats and social engineering. This aligns with previous research that emphasizes the susceptibility of cloud systems to external attacks that exploit weak credential management and phishing schemes [1][2]. Blockchain's decentralized nature, which eliminates single points of failure, appears particularly effective in mitigating these high-frequency threats, as the technology's tamper-proof record-keeping and automated verification processes can limit attackers' ability to manipulate access controls and misuse credentials [3][4].

The skewness and kurtosis analysis further highlighted the differences in the distribution of incident types, with phishing incidents exhibiting heavier tails, indicating a higher frequency of extreme events. This finding is consistent with prior studies that have shown the disproportionate impact of phishing attacks, particularly in cloud environments where sensitive data is often accessed remotely [5][6]. Blockchain's ability to create an immutable audit trail and distribute control across multiple nodes presents a compelling solution to these challenges by reducing the reliance on vulnerable, centralized systems and minimizing the risk of human error in managing credentials [7][8]. The negative correlation between incident frequency and both skewness and kurtosis reinforces this, suggesting that as the frequency of incidents increases, the distribution becomes more symmetrical and less prone to extreme, high-impact events. This outcome supports the notion that blockchain could play a key role in stabilizing cloud security environments by curbing the frequency of major breaches, a benefit that aligns with the findings of Bhushan et al. [9].

The logistic regression analysis provided compelling evidence of blockchain’s superiority over traditional security methods in mitigating cyber incidents. The significantly positive coefficient for the security measure variable demonstrated that blockchain-based frameworks outperform traditional models such as encryption and centralized access control. This is particularly important in the context of mitigating insider threats and social engineering attacks, which remain persistent challenges in cloud security due to their exploitation of human vulnerabilities [10][11]. The odds ratio of 5.75 highlights the considerable advantage that blockchain frameworks offer in reducing the likelihood of successful attacks, a finding consistent with other studies that have praised blockchain's decentralized approach to identity management and access control [12]. This is further supported by the observed decline in the effectiveness of traditional methods as incident severity increases, a result that echoes the limitations of centralized security frameworks in addressing sophisticated, high-severity threats [13]. Blockchain’s ability to automate identity verification and create tamper-resistant records of network activities provides a more robust defense, particularly in scenarios involving complex, multi-stage attacks [14][15].

Despite its clear advantages, the analysis of blockchain's scalability and performance within cloud security architectures reveals several challenges. The time series analysis of the Ethereum blockchain's performance over time showed that while transaction throughput increased significantly, the system reached a plateau at around 25 TPS. This limitation in throughput underscores the scalability concerns associated with blockchain technology, particularly in cloud environments that require the ability to handle high volumes of transactions in real-time [16] [17]. Previous studies have also highlighted this issue, noting that the computational overhead of maintaining consensus in blockchain networks, particularly those using proof-of-work mechanisms, can severely limit throughput and increase latency as transaction volumes grow [18] [19]. This performance bottleneck presents a critical barrier to the widespread adoption of blockchain in cloud environments, where low-latency, high-throughput systems are essential for maintaining operational efficiency.

The rise in network congestion and latency, as revealed by the time series analysis, further emphasizes the need for scalability solutions. As network congestion approached 95% of capacity, latency increased to 30 seconds, a significant delay that could hinder the functionality of real-time cloud applications. These findings are consistent with earlier research that has pointed to network congestion as a major factor limiting blockchain performance, particularly in systems that rely on decentralized consensus mechanisms [20]. The results highlight the need for advanced scalability solutions such as layer-2 protocols, sidechains, and sharding, which can help distribute the computational load more effectively and reduce congestion in high-demand environments [21][22]. Without these optimizations, blockchain's potential as a cloud security solution may be constrained by its inherent performance limitations.

Moreover, the comparison of start-of-year and end-of-year metrics clearly illustrated the trade-offs between throughput, latency, and network congestion. While transaction throughput improved by 67%, both latency and network congestion rose sharply, suggesting that blockchain's ability to scale is hampered by its reliance on current consensus mechanisms [23]. This mirrors findings in the literature that argues for the adoption of hybrid blockchain models, where only critical security functions are decentralized. At the same time, other processes remain centralized to ensure system efficiency [24]. Such an approach could offer a more practical solution to the scalability challenges identified in this study, enabling cloud systems to leverage blockchain's security benefits without sacrificing performance.

5. Conclusion and Recommendation

This study demonstrates that blockchain technology offers significant advantages in addressing human-network vulnerabilities within cloud environments. Its decentralized structure mitigates common issues like phishing and credential misuse by eliminating single points of failure and providing tamper-proof records. However, while blockchain outperforms traditional security methods in areas such as identity management and insider threat mitigation, its performance is limited by scalability challenges. As evidenced by the time series analysis, the technology struggles to handle high transaction volumes efficiently, with increased network congestion and latency under heavy loads. These performance constraints present a barrier to the widespread integration of blockchain in cloud environments, especially those requiring real-time data processing. To fully realize blockchain's potential as a solution for cloud security, addressing these scalability issues is essential.

1. Organizations should invest in layer-2 scaling solutions, such as sidechains and sharding, to alleviate blockchain's performance bottlenecks and ensure the system can handle higher transaction volumes.
2. A hybrid approach should be considered, where critical security processes are decentralized while less essential operations remain centralized, optimizing both security and performance.

3. Regulatory frameworks should evolve to accommodate blockchain's decentralized nature while ensuring compliance with data protection laws, particularly concerning data immutability and the right to be forgotten.
4. Further research and development into energy-efficient consensus mechanisms, like proof-of-stake, should be prioritized to reduce the environmental impact of blockchain technology in cloud security systems.

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

References

[1] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions,” *Electronics*, vol. 12, no. 6, pp. 1–42, Mar. 2023, doi: https://doi.org/10.3390/electronics12061333.

[2] M. Uddin, A. Khalique, A. K. Jumani, S. S. Ullah, and S. Hussain, “Next-Generation Blockchain-Enabled Virtualized Cloud Security Solutions: Review and Open Challenges,” *Electronics*, vol. 10, no. 20, p. 2493, Oct. 2021, doi: https://doi.org/10.3390/electronics10202493.

[3] R. Silva, H. Inácio, and R. P. Marques, “Effective and Potential Implications of Blockchain Technology for Auditing,” *Advances in Intelligent Systems and Computing*, vol. 1368, pp. 435–451, 2021, doi: https://doi.org/10.1007/978-3-030-72654-6_42.

[4] A. A.-N. Patwary *et al.*, “Towards Secure Fog Computing: A Survey on Trust Management, Privacy, Authentication, Threats and Access Control,” *Electronics*, vol. 10, no. 10, p. 1171, May 2021, doi: https://doi.org/10.3390/electronics10101171.

[5] J. Krysińska, “Breakdown of the 11 most significant 2023 data breaches,” *nordlayer.com*, Dec. 12, 2023. https://nordlayer.com/blog/data-breaches-in-2023/ (accessed Oct. 14, 2024).

[6] L. Albshaier, S. Almarri, and M. M. H. Rahman, “A Review of Blockchain’s Role in E-Commerce Transactions: Open Challenges, and Future Research Directions,” *Computers*, vol. 13, no. 1, p. 27, Jan. 2024, doi: https://doi.org/10.3390/computers13010027.

[7] A. I. Sanka and R. C. C. Cheung, “A systematic review of blockchain scalability: Issues, solutions, analysis and future research,” *Journal of Network and Computer Applications*, vol. 195, p. 103232, Dec. 2021, doi: https://doi.org/10.1016/j.jnca.2021.103232.

[8] T. Scott, “TradeLens: How IBM and Maersk Are Sharing Blockchain to Build a Global Trade Platform - THINK Blog,” *THINK Blog*, Nov. 27, 2018. https://www.ibm.com/blogs/think/2018/11/tradelens-how-ibm-and-maersk-are-sharing-blockchain-to-build-a-global-trade-platform/ (accessed Oct. 14, 2024).

[9] I. Hagui *et al.*, “A blockchain-based security system with light cryptography for user authentication security,” *Multimedia Tools and Applications*, vol. 83, Nov. 2023, doi: https://doi.org/10.1007/s11042-023-17643-5.

[10] S. Lad, “Cybersecurity Trends: Integrating AI to Combat Emerging Threats in the Cloud Era,” *Integrated Journal of Science and Technology*, vol. 1, no. 8, 2024, Accessed: Oct. 14, 2024. [Online]. Available: http://ijstindex.com/index.php/ijst/article/view/60

[11] B. Anthony Jnr., “Investigating the Decentralized Governance of Distributed Ledger Infrastructure Implementation in Extended Enterprises,” *Journal of the Knowledge Economy*, vol. 14, Oct. 2022, doi: https://doi.org/10.1007/s13132-022-01079-7.

[12] H. Omotunde and M. Ahmed, “A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond,” *Mesopotamian Journal of Cybersecurity*, 2023, doi: https://doi.org/10.58496/MJCS/2023/016.

[13] M. B. Qureshi *et al.*, “Encryption Techniques for Smart Systems Data Security Offloaded to the Cloud,” *Symmetry*, vol. 14, no. 4, p. 695, Apr. 2022, doi: https://doi.org/10.3390/sym14040695.

[14] C. S. Adigwe, O. O. Olaniyi, S. O. Olabanji, O. J. Okunleye, N. R. Mayeke, and S. A. Ajayi, “Forecasting the Future: The Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy,” *Asian journal of economics, business and accounting*, vol. 24, no. 4, pp. 126–146, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41269.

[15] M. Dawood, S. Tu, C. Xiao, H. Alasmary, M. Waqas, and S. U. Rehman, “Cyberattacks and Security of Cloud Computing: A Complete Guideline,” *Symmetry*, vol. 15, no. 11, pp. 1–33, Nov. 2023, doi: https://doi.org/10.3390/sym15111981.

[16] U. Inayat, M. Farzan, S. Mahmood, M. F. Zia, S. Hussain, and F. Pallonetto, “Insider threat mitigation: Systematic literature review,” *Ain Shams Engineering Journal*, pp. 103068–103068, Sep. 2024, doi: https://doi.org/10.1016/j.asej.2024.103068.

[17] M. Chauhan and S. Shiaeles, “An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions,” *Network*, vol. 3, no. 3, pp. 422–450, Sep. 2023, doi: https://doi.org/10.3390/network3030018.

[18] O. I. Akinola, O. O. Olaniyi, O. S. Ogungbemi, O. B. Oladoyinbo, and A. O. Olisa, “Resilience and Recovery Mechanisms for Software-Defined Networking (SDN) and Cloud Networks,” *Journal of Engineering Research and Reports*, vol. 26, no. 8, pp. 112–134, Jul. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i81234.

[19] K. Kioskli, T. Fotis, S. Nifakos, and H. Mouratidis, "The Importance of Conceptualizing the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0," *Applied Sciences*, vol. 13, no. 6, p. 3410, Jan. 2023, doi: https://doi.org/10.3390/app13063410.

[20] A. S. Arigbabu, O. O. Olaniyi, and A. Adeola, “Exploring Primary School Pupils’ Career Aspirations in Ibadan, Nigeria: A Qualitative Approach,” *Journal of Education, Society and Behavioural Science*, vol. 37, no. 3, pp. 1–16, Apr. 2024, doi: https://doi.org/10.9734/jesbs/2024/v37i31308.

[21] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, “Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain

Technology with Cloud Computing," *Future Internet*, vol. 14, no. 11, 2022, doi: https://doi.org/10.3390/fi14110341.

[22] Z. Wenhua, F. Qamar, T.-A. N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, "Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends," *Electronics*, vol. 12, no. 3, p. 546, Jan. 2023, doi: https://doi.org/10.3390/electronics12030546.

[23] A. T. Arigbabu, O. O. Olaniyi, C. S. Adigwe, O. O. Adebiyi, and S. A. Ajayi, "Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale," *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 85–107, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5441.

[24] B. Bhushan, P. Sinha, K. M. Sagayam, and A. J, "Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions," *Computers & Electrical Engineering*, vol. 90, p. 106897, Nov. 2020, doi: https://doi.org/10.1016/j.compeleceng.2020.106897.

[25] C. U. Asonze, O. S. Ogungbemi, F. A. Ezeugwa, A. O. Olisa, O. I. Akinola, and O. O. Olaniyi, "Evaluating the Trade-offs between Wireless Security and Performance in IoT Networks: A Case Study of Web Applications in AI-Driven Home Appliances," *Journal of Engineering Research and Reports*, vol. 26, no. 8, pp. 411–432, Aug. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i81255.

[26] A. Zutshi, A. Grilo, and T. Nodehi, "The value proposition of blockchain technologies and its impact on Digital Platforms," *Computers & Industrial Engineering*, vol. 155, p. 107187, May 2021, doi: https://doi.org/10.1016/j.cie.2021.107187.

[27] U. T. I. Igwenagu, A. A. Salami, A. S. Arigbabu, C. E. Mesode, T. O. Oladoyinbo, and O. O. Olaniyi, "Securing the Digital Frontier: Strategies for Cloud Computing Security, Database Protection, and Comprehensive Penetration Testing," *Journal of Engineering Research and Reports*, vol. 26, no. 6, pp. 60–75, May 2024, doi: https://doi.org/10.9734/jerr/2024/v26i61162.

[28] M. Krichen, M. Ammi, A. Mihoub, and M. Almutiq, "Blockchain for Modern Applications: A Survey," *Sensors*, vol. 22, no. 14, p. 5274, Jul. 2022, doi: https://doi.org/10.3390/s22145274.

[29] P. C. Joeaneke, T. M. Kolade, O. O. Val, A. O. Olisa, S. A. Joseph, and O. O. Olaniyi, "Enhancing Security and Traceability in Aerospace Supply Chains through Block Chain Technology," *Journal of Engineering Research and Reports*, vol. 26, no. 10, pp. 114–135, Oct. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i101294.

[30] S. Muhammad, F. Meerjat, A. Meerjat, A. Dalal, and S. Abdul, "Enhancing Cybersecurity Measures for Blockchain: Securing Transactions in Decentralized Systems," *Unique Endeavor in Business & Social Sciences*, vol. 2, no. 1, pp. 120–141, 2023, Available: https://unbss.com/index.php/unbss/article/view/53

[31] G. Balamurugan, A. K. Tyagi, and Richa, "A Survey on Privacy Preserving and Trust Building Techniques of Blockchain-Based Systems," *www.igi-global.com*, 2023. https://www.igi-global.com/chapter/a-survey-on-privacy-preserving-and-trust-building-techniques-of-blockchain-based-systems/333149 (accessed Oct. 14, 2024).

[32] P. C. Joeaneke, O. O. Val, O. O. Olaniyi, O. S. Ogungbemi, A. O. Olisa, and O. I. Akinola, "Protecting Autonomous UAVs from GPS Spoofing and Jamming: A Comparative Analysis of Detection and Mitigation Techniques," *Journal of Engineering*

Research and Reports, vol. 26, no. 10, pp. 71–92, Oct. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i101291.

[33] S. M. Idrees, M. Nowostawski, R. Jameel, and A. K. Mourya, “Security Aspects of Blockchain Technology Intended for Industrial Applications,” *Electronics*, vol. 10, no. 8, p. 951, Apr. 2021, doi: https://doi.org/10.3390/electronics10080951.

[34] R. El Sibai, N. Gemayel, J. Bou Abdo, and J. Demerjian, “A survey on access control mechanisms for cloud computing,” *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 2, Aug. 2019, doi: https://doi.org/10.1002/ett.3720.

[35] A. M. John-Otumu, C. Ikerionwu, O. O. Olaniyi, O. Dokun, U. F. Eze, and O. C. Nwokonkwo, “Advancing COVID-19 Prediction with Deep Learning Models: A Review,” *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG), Omu-Aran, Nigeria, 2024*, pp. 1–5, Apr. 2024, doi: https://doi.org/10.1109/seb4sdg60871.2024.10630186.

[36] Y. A. Marquis, T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, and S. S. Ajayi, “Proliferation of AI Tools: A Multifaceted Evaluation of User Perceptions and Emerging Trend,” *Asian Journal of Advanced Research and Reports*, vol. 18, no. 1, pp. 30–35, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i1596.

[37] A. Khanna, A. Sah, V. Bolshev, A. Burgio, V. Panchenko, and M. Jasiński, “Blockchain–Cloud Integration: A Survey,” *Sensors*, vol. 22, no. 14, p. 5238, Jul. 2022, doi: https://doi.org/10.3390/s22145238.

[38] B. Shrimali and H. B.Patel, “Blockchain State-of-the-Art: Architecture, Use Cases, Consensus, Challenges and Opportunities,” *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 9, Aug. 2021, doi: https://doi.org/10.1016/j.jksuci.2021.08.005.

[39] O. S. Ogungbemi, F. A. Ezeugwa, O. O. Olaniyi, O. I. Akinola, and O. B. Oladoyinbo, “Overcoming Remote Workforce Cyber Threats: A Comprehensive Ransomware and Bot Net Defense Strategy Utilizing VPN Networks,” *Journal of Engineering Research and Reports*, vol. 26, no. 8, pp. 161–184, Jul. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i81237.

[40] M. Abdul and S. Saleem, “Navigating Blockchain’s Twin Challenges: Scalability and Regulatory Compliance,” *Blockchains*, vol. 2, no. 3, pp. 265–298, Sep. 2024, doi: https://doi.org/10.3390/blockchains2030013.

[41] S. U. Okon, O. O. Olateju, O. S. Ogungbemi, S. A. Joseph, A. O. Olisa, and O. O. Olaniyi, “Incorporating Privacy by Design Principles in the Modification of AI Systems in Preventing Breaches across Multiple Environments, Including Public Cloud, Private Cloud, and On-prem,” *Journal of Engineering Research and Reports*, vol. 26, no. 9, pp. 136–158, Sep. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i91269.

[42] H. Jin and J. Xiao, “Towards trustworthy blockchain systems in the era of ‘Internet of value’: development, challenges, and future trends,” *Science China Information Sciences*, vol. 65, no. 5, Oct. 2021, doi: https://doi.org/10.1007/s11432-020-3183-0.

[43] J. Zarrin, H. Wen Phang, L. Babu Saheer, and B. Zarrin, “Blockchain for decentralization of internet: prospects, trends, and challenges,” *Cluster Computing*, vol. 1, no. 1, May 2021, doi: https://doi.org/10.1007/s10586-021-03301-8.

[44] S. O. Olabanji, Y. A. Marquis, C. S. Adigwe, A. S. Abidemi, T. O. Oladoyinbo, and O. O. Olaniyi, “AI-Driven Cloud Security: Examining the Impact of User Behavior

Analysis on Threat Detection," *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 57–74, Jan. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3424.

[45] C. Daah, A. Qureshi, I. Awan, and S. Konur, "Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework," *Electronics*, vol. 13, no. 5, p. 865, Jan. 2024, doi: https://doi.org/10.3390/electronics13050865.

[46] R. Kumar and R. Sharma, "Leveraging blockchain for ensuring trust in IoT: A survey," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, Sep. 2021, doi: https://doi.org/10.1016/j.jksuci.2021.09.004.

[47] T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, O. O. Adebiyi, O. J. Okunleye, and A. I. Alao, "Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics," *Asian Journal of Advanced Research and Reports*, vol. 18, no. 2, pp. 1–23, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i2601.

[48] E. I. Zafir *et al.*, "Enhancing security of Internet of Robotic Things: A review of recent trends, practices, and recommendations with encryption and blockchain techniques," *Internet of Things*, vol. 28, p. 101357, Dec. 2024, doi: https://doi.org/10.1016/j.iot.2024.101357.

[49] J. Louw-Reimer, J. L. M. Nielsen, N. Bjørn-Andersen, and N. Kouwenhoven, "Boosting the Effectiveness of Containerised Supply Chains: A Case Study of TradeLens," *Progress in IS*, pp. 95–115, 2021, doi: https://doi.org/10.1007/978-3-030-72785-7_6.

[50] O. O. Olaniyi, "Ballots and Padlocks: Building Digital Trust and Security in Democracy through Information Governance Strategies and Blockchain Technologies," *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 172–189, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5447.

[51] M. R. Dorsala, V. N. Sastry, and S. Chapram, "Blockchain-based solutions for cloud computing: A survey," *Journal of Network and Computer Applications*, vol. 196, p. 103246, Dec. 2021, doi: https://doi.org/10.1016/j.jnca.2021.103246.

[52] O. O. Olaniyi, F. A. Ezeugwa, C. G. Okatta, A. S. Arigbabu, and P. C. Joeaneke, "Dynamics of the Digital Workforce: Assessing the Interplay and Impact of AI, Automation, and Employment Policies," *Archives of current research international*, vol. 24, no. 5, pp. 124–139, Apr. 2024, doi: https://doi.org/10.9734/acri/2024/v24i5690.

[53] S. Shukla, Mohd. F. Hassan, D. C. Tran, R. Akbar, I. V. Paputungan, and M. K. Khan, "Improving latency in Internet-of-Things and cloud computing for real-time data transmission: a systematic literature review (SLR)," *Cluster Computing: The Journal of Networks, Software Tools and Applications*, vol. 26, p. 1, 2021, doi: https://doi.org/10.1007/s10586-021-03279-3.

[54] D. L. L. Moura, A. L. L. Aquino, and A. A. F. Loureiro, "An edge computing and distributed ledger technology architecture for secure and efficient transportation," *Ad Hoc Networks*, vol. 164, p. 103633, Nov. 2024, doi: https://doi.org/10.1016/j.adhoc.2024.103633.

[55] O. O. Olaniyi, O. O. Olaoye, and O. J. Okunleye, "Effects of Information Governance (IG) on Profitability in the Nigerian Banking Sector," *Asian Journal of Economics, Business and Accounting*, vol. 23, no. 18, pp. 22–35, Jul. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i181055.

[56] M. A. F. Noor and K. Mustafa, “A taxonomy of endpoint vulnerabilities and affected blockchain architecture layers,” *Concurrency and Computation Practice and Experience*, vol. 36, no. 19, May 2024, doi: https://doi.org/10.1002/cpe.8158.
[57] O. O. Olaniyi, O. O. Omogoroye, F. G. Olaniyi, A. I. Alao, and T. O. Oladoyinbo, “CyberFusion Protocols: Strategic Integration of Enterprise Risk Management, ISO 27001, and Mobile Forensics for Advanced Digital Security in the Modern Business Ecosystem,” *Journal of Engineering Research and Reports*, vol. 26, no. 6, p. 32, 2024, doi: https://doi.org/10.9734/JERR/2024/v26i61160.
[58] D. Schönle, K. Wallis, J. Stodt, C. Reich, D. Welte, and A. Sikora, “Industry Use Cases on Blockchain Technology,” *Industry Use Cases on Blockchain Technology Applications in IoT and the Financial Sector*, 2021. https://www.igi-global.com/chapter/industry-use-cases-on-blockchain-technology/273818 (accessed Oct. 14, 2024).
[59] O. O. Olaniyi, J. C. Ugonnia, F. G. Olaniyi, A. T. Arigbabu, and C. S. Adigwe, “Digital Collaborative Tools, Strategic Communication, and Social Capital: Unveiling the Impact of Digital Transformation on Organizational Dynamics,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 140–156, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5444.
[60] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, “Blockchain smart contracts: Applications, challenges, and future trends,” *Peer-to-Peer Networking and Applications*, vol. 14, no. 1, pp. 2901–2925, Apr. 2021, doi: https://doi.org/10.1007/s12083-021-01127-0.
[61] O. O. Olateju, S. U. Okon, U. T. I. Igwenagu, A. A. Salami, T. O. Oladoyinbo, and O. O. Olaniyi, “Combating the Challenges of False Positives in AI-Driven Anomaly Detection Systems and Enhancing Data Security in the Cloud,” *Asian Journal of Research in Computer Science*, vol. 17, no. 6, pp. 264–292, Jun. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i6472.
[62] A. R. Sai, J. Buckley, B. Fitzgerald, and A. L. Gear, “Taxonomy of centralization in public blockchain systems: A systematic literature review,” *Information Processing & Management*, vol. 58, no. 4, p. 102584, Jul. 2021, doi: https://doi.org/10.1016/j.ipm.2021.102584.
[63] O. O. Olateju, S. U. Okon, O. O. Olaniyi, A. D. Samuel-Okon, and C. U. Asonze, “Exploring the Concept of Explainable AI and Developing Information Governance Standards for Enhancing Trust and Transparency in Handling Customer Data,” *Journal of Engineering Research and Reports*, vol. 26, no. 7, pp. 244–268, Jun. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i71206.
[64] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, “A privacy-preserving traceability system for self-sovereign identity-based inter-organizational business processes,” *Computer Standards & Interfaces*, vol. 92, pp. 103930–103930, Sep. 2024, doi: https://doi.org/10.1016/j.csi.2024.103930.
[65] A. A. Salami, U. T. I. Igwenagu, C. E. Mesode, O. O. Olaniyi, and O. B. Oladoyinbo, “Beyond Conventional Threat Defense: Implementing Advanced Threat Modeling Techniques, Risk Modeling Frameworks and Contingency Planning in the Healthcare Sector for Enhanced Data Security,” *Journal of Engineering Research and Reports*, vol. 26, no. 5, pp. 304–323, Apr. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i51156.

[66] A. D. Samuel-Okon, O. I. Akinola, O. O. Olaniyi, O. O. Olateju, and S. A. Ajayi, “Assessing the Effectiveness of Network Security Tools in Mitigating the Impact of Deepfakes AI on Public Trust in Media,” *Archives of Current Research International*, vol. 24, no. 6, pp. 355–375, Jul. 2024, doi: https://doi.org/10.9734/acri/2024/v24i6794.
[67] L. Alevizos, V. T. Ta, and M. Hashem Eiza, “Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review,” *Security and Privacy*, vol. 5, no. 1, Nov. 2021, doi: https://doi.org/10.1002/spy2.191.
[68] A. D. Samuel-Okon, O. O. Olateju, S. U. Okon, O. O. Olaniyi, and U. T. I. Igwenagu, “Formulating Global Policies and Strategies for Combating Criminal Use and Abuse of Artificial Intelligence,” *Archives of current research international*, vol. 24, no. 5, pp. 612–629, Jun. 2024, doi: https://doi.org/10.9734/acri/2024/v24i5735.
[69] J. C. Ugonnia, O. O. Olaniyi, F. G. Olaniyi, A. A. Arigbabu, and T. O. Oladoyinbo, “Towards Sustainable IT Infrastructure: Integrating Green Computing with Data Warehouse and Big Data Technologies to Enhance Efficiency and Environmental Responsibility,” *Journal of Engineering Research and Reports*, vol. 26, no. 5, pp. 247–261, Apr. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i51151.
[70] Y. Merrad *et al.*, “Blockchain: Consensus Algorithm Key Performance Indicators, Trade-Offs, Current Trends, Common Drawbacks, and Novel Solution Proposals,” *Mathematics*, vol. 10, no. 15, p. 2754, Jan. 2022, doi: https://doi.org/10.3390/math10152754.
[71] K. M. Khan, J. Arshad, W. Iqbal, S. Abdullah, and H. Zaib, “Blockchain-enabled real-time SLA monitoring for cloud-hosted services,” *Cluster Computing*, vol. 25, Oct. 2021, doi: https://doi.org/10.1007/s10586-021-03416-y.
[72] M. Rukhiran, S. Boonsong, and P. Netinant, “Sustainable Optimizing Performance and Energy Efficiency in Proof of Work Blockchain: A Multilinear Regression Approach,” *Sustainability*, vol. 16, no. 4, pp. 1519–1519, Feb. 2024, doi: https://doi.org/10.3390/su16041519.
[73] B. Rana, Y. Singh, and P. K. Singh, “A systematic survey on internet of things: Energy efficiency and interoperability perspective,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 8, Dec. 2020, doi: https://doi.org/10.1002/ett.4166.
[74] S. Grabowska and S. Saniuk, “Assessment of the Competitiveness and Effectiveness of an Open Business Model in the Industry 4.0 Environment,” *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 8, no. 1, p. 57, Mar. 2022, doi: https://doi.org/10.3390/joitmc8010057.
[75] A. Arabsorkhi and E. Khazaei, “Blockchain Technology and GDPR Compliance: A Comprehensive Applicability Model,” *International Journal of Web Research*, vol. 7, no. 2, pp. 49–63, Apr. 2024, doi: https://doi.org/10.22133/ijwr.2024.459490.1221.